

**Phil Keown**  
Engagement Lead  
T: 020 7728 2394  
E: philip.r.keown@uk.gt.com

**Paul Eckersley**  
Manager  
T: 0113 200 2525  
E: paul.j.eckersley@uk.gt.com

**Aparna Muthurajagopalan**  
Executive  
T: 020 78652264  
E: aparna.muthurajagopalan@uk.gt.com

## Information Commissioner's Office

### Internal Audit 2015-16: IT Asset Management Review – Phase 1

Last updated 11 May 2017

Distribution		Timetable	
For action	Head of Customer and Business Services	Fieldwork completed	7 November 2016
		Draft report issued	28 November 2016
For information	Senior Corporate Officer Audit Committee	Management comments	16 December 2016
		Final report issued	19 December 2016

# Contents

Sections	Glossary
<b>1 Executive Summary</b>	<b>1 ACCSEC</b> Accountable security (encrypted) devices
<b>2 Detailed Findings</b>	<b>3 ALMO</b> Asset and Licence Management Officer
<b>Appendices</b>	<b>CESG</b> Communications Electronics Security Group (the UK Government's national technical authority for information assurance)
<b>A Internal audit approach</b>	<b>6 Custodian</b> Person responsible for managing encryption systems
<b>B Definition of internal audit opinion and ratings</b> Bookmark not defined.	Error! <b>IGSG</b> Information Governance Security Group – body that oversees information security

This report is confidential and is intended for use by the management and Directors of ICO only. It forms part of our continuing dialogue with you. It should not be made available, in whole or in part, to any third party without our prior written consent. We do not accept responsibility for any reliance that third parties may place upon this report. Any third party relying on this report does so entirely at its own risk. We accept no liability to any third party for any loss or damage suffered or costs incurred, arising out of or in connection with the use of this report, however such loss or damage is caused.

It is the responsibility solely of ICO's management to ensure that there are adequate arrangements in place in relation to risk management, governance and control.

# 1 Executive Summary

## 1.1 Background

As part of the 2016-17 Internal Audit Plan, we have agreed with management and the Audit Committee to undertake a review to provide assurance over the process to manage IT assets. Following an incident involving a missing (secure) laptop, a review was requested by the Audit Committee over the controls over Accountable Security devices (called the “Cryptographic Controls” review). The ICO is also implementing a revised process to manage all IT assets going forward. This review focuses on how IT assets are managed and controlled but does not cover the specific requirements for compliance with CESG requirements.

## 1.2 Scope

The objectives of the review are to provide assurance over the adequacy of controls over the management of IT assets. The findings and conclusions from this review will support our annual opinion to the Audit Committee on the adequacy and effectiveness of governance arrangements. The review will be delivered in two phases:

- 1 An assessment of the design of the IT asset management processes to provide to identify opportunities for improvement; and
- 2 Review of the operational processes based upon the new set of IT asset management controls reviewed in phase 1.

This report relates to the first of the two phases, i.e. the design of new controls and processes which will be introduced. Our review considered the following risks:

- IT assets are missing and are unknown to ICO management
- The loss of an IT asset may contain sensitive information which could result in reputational damage
- Asset re-use / redeployment is poor leading to ICO purchasing additional assets and therefore increasing costs
- Unauthorised procurement lead to additional time spent managing and integrating the unauthorised asset

Further details on responsibilities, approach and scope are included in Appendix A.

## 1.3 Overall conclusion

### Overall assessment – Design Effectiveness

We have identified matters which, if resolved, will help management fulfil their responsibility to maintain a robust system of internal control.

**Green**

Please refer to appendix B for further information regarding our overall assessment and audit finding ratings.

The table details the key findings from our review.

#### 1.4 Key findings

Risk / Process	High	Medium	Low	Imp.
IT asset management	-	1	-	-
IT asset procurement	-	-	1	-
IT asset usage	-	-	1	-
<b>Total</b>	-	<b>1</b>	<b>2</b>	-

There are no high rated findings arising out of our review and we identified one medium rated finding; IT assets are not reconciled between an independent source such as an invoice or delivery note and the IT assets at the ICO.

Further details of our findings and recommendations are provided in Section 2.

#### 1.5 Basis of opinion

We identified the following good practices:

- One person has responsibility for all physical IT assets and records
- Software asset manager post in place
- Formal procurement process in place for projects
- Management structure in place to oversee IT asset governance

#### 1.6 Acknowledgement

We would like to take this opportunity to thank the staff involved for their co-operation during this internal audit.

## 2 Detailed Findings

### 2.1 IT asset management

1.	Medium	Accurate and complete asset records are not in place
Finding and Implication	Proposed action	Agreed action (Date / Ownership)
<p>On a bi-annual basis the ALMO conducts a physical audit of all IT assets except ACCSEC devices. ACCSEC devices are covered as part of the annual ACCSEC audit carried out by the Custodian to meet CESG requirements. The results of the physical audit are not being formally captured or reported to management. Additionally, although the non-ACCSEC assets are subject to a physical audit and the results of that audit are reconciled against the ICO asset register spreadsheet, there is no reconciliation against an independent source of asset information, such as an invoice or delivery note.</p> <p>Asset management policies states that should any issues be identified as part of the audit, these should be raised with the IT Helpdesk and decisions are made on next steps is made by the business based on the criticality of the incident. The policy does not state how this assessment of criticality should be carried out.</p> <p>Asset record keeping that is not operating effectively undermines the accuracy of a physical asset count which can in turn mean that assets that may be lost or stolen are not identified in a timely manner leading to damage to the ICO's reputation.</p>	<p>The results of physical audits should be recorded within the asset register (when was the last physical audit conducted and by who) and shared with the IGSG.</p> <p>The incident management process over lost or stolen assets to include how to assess the criticality and therefore the appropriate action to take.</p>	<p><i>Physical audit log to be added to asset register. Once each physical audit is complete, record to be copied from asset register and held as a stand-alone record of that periods' physical asset check. Reference to this to be added to the Asset Management procedure V1.0</i></p> <p><i>Asset Management procedure V1.0 to be updated to include risk assessment and action plan</i></p> <p><i>Date Effective: Complete by 31 January 2017 to enable phase II review of the operational processes referred to in 1.2 above.</i></p> <p><i>Owner: Emma Deen</i></p>

## 2.2 IT asset procurement

2.	Low	Lack of guidance on non-project IT procurement
Finding and Implication	Proposed action	Agreed action (Date / Ownership)
<p>The ICO utilises the project management process to introduce new technology or make any significant changes to existing technologies. Under project management governance, purchases of equipment are made which are subject to management approval. IT assets that are not requested as part of a project (such as mice and keyboards) do not have a formal procurement process to follow. We identified that asset procurement can be initiated in three ways:</p> <ol style="list-style-type: none"> <li>1. As a result of a new project</li> <li>2. Replacing an asset as a result of end of life or damage</li> <li>3. Other ad-hoc equipment requests</li> </ol> <p>Assets that are procured for a project will go through the formal project management governance and are approved by the project board. Other IT asset purchases are reviewed IT Service Team Manager and approved by the Group Manager, Business Development.</p> <p>Most IT equipment purchases are raised with ICO's approved suppliers, Northgate or SEC. However, we noted that where purchases are made for low value items (such as a keyboard or a mouse), the purchase can be made with a different supplier. It is not clear what can be purchased outside of the formal IT procurement process or how.</p> <p>We were informed that where assets are not procured with approved suppliers (such as Northgate and SCC), ensuring that ICO's technical standards are being adhered to is the responsibility of Group Manager, Business Development.</p>	<p>The process for non-project asset procurement should be documented and sets out what can be purchased, from where and who has the authority to approve such purchases.</p>	<p><i>Non-project IT procurement process to be documented and shared with those with delegated authority</i></p> <p><i>Date Effective: 31 January 2017</i></p> <p><i>Owner: Emma Deen</i></p>

## 2.3 IT asset usage

3.	Low	<b>Monitoring of IT assets not connected to the network</b>
----	-----	---

Finding and Implication	Proposed action	Agreed action ( <i>Date / Ownership</i> )
<p>Monitoring is not in place on all devices to identify ICO IT assets that have not been connected to the network for an appropriate period of time. Such devices may be candidates for redeployment or lack of connection may indicate that an asset has been lost or stolen.</p> <p>Management are reviewing their IT Service Desk system solution and a new system could incorporate asset monitoring.</p>	<p>Management should ensure that monitoring is in place to identify that ICO IT equipment is in active use.</p>	<p><i>It was explained during the audit that ICO are limited in what they can do to monitor hardware use via network activity. We don't have direct control over this because of our contractual relationship with Northgate Public Services. Desktop management tools enable asset monitoring via Active Directory which ICO cannot utilise.</i></p> <p><i>The RSA portal reports enable us to monitor home working log in frequency. This will allow us to identify staff who haven't logged in via their allocated device for an extended period of time. Report to be added to monthly monitoring.</i></p> <p><i>Replacement IT service desk requirement checklist to include system monitoring abilities as a 'should have' requirement.</i></p> <p><i>Date Effective: 31 January 2017</i></p> <p><i>Owner: Emma Deen</i></p>

## A Internal audit approach

### Approach

Our audit will be carried out in accordance with the guidance contained within the Public Sector Internal Audit Standards (2013), and the Auditing Practices Board's 'Guidance for Internal Auditors'.

The objectives of the review are to provide assurance over the adequacy of controls over IT assets, in the following areas:

- Procurement of IT assets is limited to members of IT management, to ensure control is maintained over the incoming IT assets.
- All IT assets are recorded with the details pertaining to that asset (such as value, owner, location, serial number and asset number) and a process is in place to ensure IT assets' information is kept up to date
- Assets are regularly physically identified and asset records are reconciled
- ICO has the ability to determine market price for IT assets to ensure value for money
- Processes are in place to manage software licences (available licences are recorded, usage is regularly captured and available licences are used before purchasing new licences)
- Use of software is in line with licence agreement
- Renewal dates for licence agreements are documented) and responsibility for software licence renewal is in place
- Reporting of assets periodically to senior management

- A process is in place to ensure unauthorised equipment or assets are identified and that IT establish the underlying reasons why this has happened

We achieved our audit objectives by:

- agreeing the principles and benefits of effective risk management arrangements with management;
- meeting with key staff to gain an understanding of the arrangements in place, building upon the information we have already gained through our audit planning process;
- reviewing key documents that support the processes in place; and
- comparing existing arrangements with established best practice and other guidance.

The findings and conclusions from this review will support our annual opinion to the Audit Committee on the adequacy and effectiveness of internal control arrangements.

## Additional information

### Client staff

The following staff were consulted as part of this review:

- Christopher Goode, Asset and Licence Management Officer
- Julie Tornetta, IT Service Team Manager
- Emma Deen, Group Manager, Business Development

### Documents received

The following documents were received during the course of this audit:

- 1 Asset management register
- 2 Software licence register
- 3 Asset management procedure
- 4 Example IT Asset changes email
- 5 Presentation on secure disposal to ICO staff
- 6 Homeworking kit process

### Locations

We visited The Information Commissioner's Office, Wilmslow for this review.

## Overall assessment and audit issues ratings

### Overall assessment

Rating	Description
<b>Red</b>	Following agreement of the nature and significance of individual issues with management, in our view this report contains matters which should be raised with Senior Management and the Audit Committee at the earliest opportunity.
<b>Amber</b>	Following agreement of the nature and significance of individual issues with management, in our view this report contains matters which require the attention of management to resolve and report on progress in line with current follow up processes.
<b>Green</b>	We have identified matters which, if resolved, will help management fulfil their responsibility to maintain a robust system of internal control.

### Audit issue rating

Within each report, every audit issue is given a rating.

Rating	Description	Features
<b>High</b>	Findings that are fundamental to the management of risk in the business area, representing a weakness in control that requires the immediate attention of management	<ul style="list-style-type: none"> <li>• Key control not designed or operating effectively</li> <li>• Potential for fraud identified</li> <li>• Non compliance with key procedures / standards</li> <li>• Non compliance with regulation</li> </ul>
<b>Medium</b>	Important findings that are to be resolved by line management.	<ul style="list-style-type: none"> <li>• Impact is contained within the department and compensating controls would detect errors</li> <li>• Possibility for fraud exists</li> <li>• Control failures identified but not in key controls</li> <li>• Non compliance with procedures / standards (but not resulting in key control failure)</li> </ul>
<b>Low</b>	Findings that identify non-compliance with established procedures.	<ul style="list-style-type: none"> <li>• Minor control weakness</li> <li>• Minor non compliance with procedures / standards</li> </ul>
<b>Improvement</b>	Items requiring no action but which may be of interest to management or best practice advice	<ul style="list-style-type: none"> <li>• Information for department management</li> <li>• Control operating but not necessarily in accordance with best practice</li> </ul>



**Grant Thornton**

An instinct for growth<sup>TM</sup>

© 2017 Grant Thornton UK LLP. All rights reserved

“Grant Thornton” refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires.

Grant Thornton UK LLP is a member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.

**[grant-thornton.co.uk](http://grant-thornton.co.uk)**

